EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	(modular exponentiation AND asymmetrical cryptosystem AND modulus AND ex ponent AND private key AND quantity AND equal$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/03/09 16:23
L3	287	(708/492).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/09 16:47
L4	265	(708/491).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/09 16:47
L5	286	(380/282).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/09 16:47
L8	140	(708/205).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/09 16:56
L9	5	Chinese Residue Theorem	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	OFF	2007/03/09 17:08
L10	0	Chinese Residue Theorem and RCA	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/03/09 17:02

EAST Search History

L11	1	Chinese Residue Theorem and decrypt$4 and encryp$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/03/09 17:03
L12	1	"5991415".pn.	USPAT	OR	OFF	2007/03/09 17:03
L15	199	(380/285).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/09 17:20
L16	1232	(380/30).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/09 17:20
S1	3694	Seifert.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/09 14:55
S2	0	Seifert-Jean.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/05 13:52
S3	5	Velten-Joachim.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/09 17:12
S4	3	"7016500".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/05 14:29

EAST Search History

S5	4	"789373".ap.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/09 16:23

Interference search

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	(modular exponentiation AND asymmetrical cryptosystem AND modulus AND ex ponent AND private key AND quantity AND equal$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/03/09 16:23

Search Results

BROWSE SEARCH IEEE XPLORE GUIDE

Results for "(chinese residue theorem or crt <in>metadata)" e-mail
Your search matched **713** of **1516137** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

(chinese residue theorem or crt <in>metadata) Search

☐ Check to search only within this results set

Display Format: ◉ Citation ○ Citation & Abstract

view selected items **Select All** **Deselect All** **View: 1-25** | 26-5

☐ **1. Residue-to-binary converters based on new Chinese remainder theorems**
Yuke Wang;
Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactic
Circuits and Systems II: Express Briefs, IEEE Transactions on]
Volume 47, Issue 3, March 2000 Page(s):197 - 205
Digital Object Identifier 10.1109/82.826745
AbstractPlus | References | Full Text: PDF(236 KB) **IEEE JNL**
Rights and Permissions

☐ **2. Cardiac resynchronization therapy**
Panescu, D.;
Engineering in Medicine and Biology Magazine, IEEE
Volume 24, Issue 2, March-April 2005 Page(s):22 - 26
Digital Object Identifier 10.1109/MEMB.2005.1411342
AbstractPlus | References | Full Text: PDF(604 KB) **IEEE JNL**
Rights and Permissions

☐ **3. A CRT-RSA Algorithm Secure against Hardware Fault Attacks**
Sining Liu; King, B.; Wei Wang;
Dependable, Autonomic and Secure Computing, 2nd IEEE International Symp
Sept. 2006 Page(s):51 - 60
Digital Object Identifier 10.1109/DASC.2006.5
AbstractPlus | Full Text: PDF(166 KB) **IEEE CNF**
Rights and Permissions

☐ **4. A CRT picture design based on plant images by nuclear power plant ope**
Kawano, R.; Ohtsuka, T.;
Systems, Man, and Cybernetics, 1999. IEEE SMC '99 Conference Proceeding
International Conference on
Volume 5, 12-15 Oct. 1999 Page(s):726 - 731 vol.5
Digital Object Identifier 10.1109/ICSMC.1999.815641
AbstractPlus | Full Text: PDF(496 KB) **IEEE CNF**
Rights and Permissions

☐ **5. Design principle and variant structure of a controllable reactor of transfo**
Mingxing Tian; Feng Zhao;
Electrical Machines and Systems, 2005. ICEMS 2005. Proceedings of the Eigh
Conference on

Volume 3, 27-29 Sept. 2005 Page(s):1780 - 1783 Vol. 3
AbstractPlus | Full Text: PDF(1384 KB) **IEEE CNF**
Rights and Permissions

6. **Characteristics and scanning circuit of Camel CRT**
Hongqing Zhu; Miaokang Wang; Biaolin Huang;
Vacuum Electronics Conference, 2002. IVEC 2002. Third IEEE International
23-25 April 2002 Page(s):276 - 277
Digital Object Identifier 10.1109/IVELEC.2002.999377
AbstractPlus | Full Text: PDF(255 KB) **IEEE CNF**
Rights and Permissions

7. **Novel method for CRT display ITC measurement**
Chuang, C.; Hong, R.; Tsai, J.;
Information Display, 1999. ASID '99. Proceedings of the 5th Asian Symposium
17-19 March 1999 Page(s):239 - 243
Digital Object Identifier 10.1109/ASID.1999.762754
AbstractPlus | Full Text: PDF(448 KB) **IEEE CNF**
Rights and Permissions

8. **A review of the current status of the CRT and likely future trends**
Woodcock, S.;
Graphic Display Devices, IEE Colloquium on
8 May 1989 Page(s):1/1
AbstractPlus | Full Text: PDF(60 KB) **IET CNF**

9. **Analysis of shadow mask thermal deformation and prediction of beam la color CRT**
Kug Woon Kim; Nam Woong Kim; Dae-Jin Kang;
Consumer Electronics, IEEE Transactions on
Volume 44, Issue 2, May 1998 Page(s):442 - 450
Digital Object Identifier 10.1109/30.681963
AbstractPlus | Full Text: PDF(748 KB) **IEEE JNL**
Rights and Permissions

10. **Development of advanced CRT disassembly technology**
Geskin, E.S.; Goldenberg, B.; Caudill, R.;
Electronics and the Environment, 2002 IEEE International Symposium on
6-9 May 2002 Page(s):249 - 253
Digital Object Identifier 10.1109/ISEE.2002.1003274
AbstractPlus | Full Text: PDF(584 KB) **IEEE CNF**
Rights and Permissions

11. **Modulation transfer function of very high resolution miniature cathode ra**
Bedell, R.J.;
Electron Devices, IEEE Transactions on
Volume 22, Issue 9, Sep 1975 Page(s):793 - 796
AbstractPlus | Full Text: PDF(472 KB) **IEEE JNL**
Rights and Permissions

12. **Perfect flat CRT discussed from a standpoint of "viewing performance"**
Saito, T.;
Consumer Electronics, IEEE Transactions on
Volume 44, Issue 3, Aug. 1998 Page(s):712 - 717
Digital Object Identifier 10.1109/30.713186
AbstractPlus | References | Full Text: PDF(428 KB) **IEEE JNL**
Rights and Permissions

13. **RSA speedup with Chinese remainder theorem immune against hardware cryptanalysis**
Sung-Ming Yen; Seungjoo Kim; Seongan Lim; Sang-Jae Moon;
Computers, IEEE Transactions on
Volume 52, Issue 4, April 2003 Page(s):461 - 472
Digital Object Identifier 10.1109/TC.2003.1190587
AbstractPlus | References | Full Text: PDF(518 KB) **IEEE JNL**
Rights and Permissions

14. **A novel vision system for CRT panel auto-inspection**
Der-Baau Perng; Cheng-Chuan Chou; Wei-Yu Chen;
Mechatronics, 2005. ICM '05. IEEE International Conference on
10-12 July 2005 Page(s):622 - 625
AbstractPlus | Full Text: PDF(239 KB) **IEEE CNF**
Rights and Permissions

15. **Efficient multi-prime RSA immune against hardware fault attack**
Yang, Y.; Abid, Z.; Wang, W.; Zhang, Z.; Yang, C.;
Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on
23-26 May 2005 Page(s):4649 - 4652 Vol. 5
Digital Object Identifier 10.1109/ISCAS.2005.1465669
AbstractPlus | Full Text: PDF(168 KB) **IEEE CNF**
Rights and Permissions

16. **A CSCW method for designing CRT correcting lens**
Yuxiu Cao; Xipeng Tong; Xiaosong Yang; Long Tang;
Computer Supported Cooperative Work in Design, 2002. The 7th International
25-27 Sept. 2002 Page(s):189 - 192
Digital Object Identifier 10.1109/CSCWD.2002.1047681
AbstractPlus | Full Text: PDF(309 KB) **IEEE CNF**
Rights and Permissions

17. **Handoff traffic distribution in cellular networks**
Zeng, H.; Chlamtac, I.;
Wireless Communications and Networking Conference, 1999. WCNC. 1999 IE
21-24 Sept. 1999 Page(s):413 - 417 vol.1
Digital Object Identifier 10.1109/WCNC.1999.797858
AbstractPlus | Full Text: PDF(404 KB) **IEEE CNF**
Rights and Permissions

18. **Contrast mapping and evaluation for electronic X-ray images on CRT dis**
Suzuki, J.; Furukawa, I.; Ono, S.; Kitamura, M.; Ando, Y.;
Medical Imaging, IEEE Transactions on
Volume 16, Issue 6, Dec. 1997 Page(s):772 - 784
Digital Object Identifier 10.1109/42.650874
AbstractPlus | References | Full Text: PDF(252 KB) **IEEE JNL**
Rights and Permissions

19. **Life-cycle environmental impacts of CRT and LCD desktop monitors**
Socolof, M.L.; Overly, J.G.; Kincaid, L.E.; Dhingra, R.; Singh, D.; Hart, K.M.;
Electronics and the Environment, 2001. Proceedings of the 2001 IEEE Interna on
7-9 May 2001 Page(s):119 - 127
Digital Object Identifier 10.1109/ISEE.2001.924513
AbstractPlus | Full Text: PDF(580 KB) **IEEE CNF**
Rights and Permissions

20. **A new CSCW prototype system for color CRT CAD/CAM**
Yuxin Cao; Chunxiao Xing; Long Tang; Lizhu Zhou;

Computer Supported Cooperative Work in Design, The Sixth International Con
12-14 July 2001 Page(s):542 - 545
Digital Object Identifier 10.1109/CSCWD.2001.942320

AbstractPlus | Full Text: PDF(224 KB) **IEEE CNF**
Rights and Permissions

☐ **21. A Java-based system for remote correction of CRT color distortion**
Abrardo, A.; Barni, M.; Cappellini, V.; Zappalorti, M.; Fabiani, L.;
Multimedia Signal Processing, 1999 IEEE 3rd Workshop on
13-15 Sept. 1999 Page(s):673 - 678
Digital Object Identifier 10.1109/MMSP.1999.793943

AbstractPlus | Full Text: PDF(344 KB) **IEEE CNF**
Rights and Permissions

☐ **22. CRT disposition: an assessment of limitations and opportunities in reuse and recycling in the U.S**
Mizuki, C.; Pitts, G.; Aanstoos, T.; Nichols, S.;
Electronics and the Environment, 1997. ISEE-1997., Proceedings of the 1997 International Symposium on
5-7 May 1997 Page(s):73 - 78
Digital Object Identifier 10.1109/ISEE.1997.605265

AbstractPlus | Full Text: PDF(660 KB) **IEEE CNF**
Rights and Permissions

☐ **23. Radiated emission from CRT of computer VDU**
Han Fang;
Electromagnetic Compatibility, 1990. Symposium Record. 1990 IEEE Internati on
21-23 Aug. 1990 Page(s):58 - 61
Digital Object Identifier 10.1109/ISEMC.1990.252732

AbstractPlus | Full Text: PDF(524 KB) **IEEE CNF**
Rights and Permissions

☐ **24. Perspectives on Small, Flat Video Displays**
Pierce, D.G.; Levy, R.A.;
Consumer Electronics, IEEE Transactions on
Volume CE-24, Issue 4, Nov. 1978 Page(s):571 - 582
Digital Object Identifier 10.1109/TCE.1978.266979

AbstractPlus | Full Text: PDF(2593 KB) **IEEE JNL**
Rights and Permissions

☐ **25. Is CRT glass-to-lead recycling safe and environmentally friendly?**
Weitzman, D.H.;
Electronics and the Environment, 2003. IEEE International Symposium on
19-22 May 2003 Page(s):329 - 334
Digital Object Identifier 10.1109/ISEE.2003.1208099

AbstractPlus | Full Text: PDF(431 KB) **IEEE CNF**
Rights and Permissions

View: 1-25 | 26-5

Help Contact Us Privacy & :

Home | Login | Logout | Access Information | Alerts

Welcome United States Patent and Trademark Office

Author Search

BROWSE SEARCH IEEE XPLORE GUIDE

OPTION 1
Quick Find an Author:
Enter a name to locate articles written by that author.

jean-pierre selfert

Example: Enter Lockett S to obtain a list of authors with the last name Lockett and the first initial S.

OPTION 2
Browse alphabetically

Select a letter from the list.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

No Authors found beginning with letter: jean-pierre selfert

Help Contact Us Privacy &

Home | Login | Logout | Access Information | Alerts

Welcome United States Patent and Trademark Office

Author Search

BROWSE SEARCH IEEE XPLORE GUIDE

OPTION 1
Quick Find an Author:
Enter a name to locate articles written by that author.

joachim velten

Example: Enter Lockett S to obtain a list of authors with the last name Lockett and the first initial S.

OPTION 2
Browse alphabetically

Select a letter from the list.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

No Authors found beginning with letter: joachim velten

Help Contact Us Privacy &

Indexed by Inspec

STIC Search Report
EIC 2100

STIC Database Tracking Number: 217524

TO: April Shan
Location: RND 2A14
Art Unit: 2135
Friday, March 09, 2007

Case Serial Number: 10/789373

From: Ruth E. Spink
Location: EIC 2100
RND-4B31
Phone: 23524

Ruth.spink@uspto.gov

Search Notes

April– Attached is the inventor, foreign patent and NPL search for the above referenced case. Be sure to contact me if you wish to refocus this search.

Ruth

Search and Information Resources Administration

Inventors
Patents

```
Set      Items    Description
S1         286    S AU=(SEIFERT, J? OR SEIFERT J?)
S2          24    S AU=(VELTEN, J? OR VELTEN J?)
S3         307    S S1 OR S2
S4         122    S S3 AND IC=(G06F OR H04L)
S5       36342    S (PUBLIC OR SECRET OR PRIVATE OR ENCRYPT? OR CRYPT?)()KEY? ? OR PKI OR
CRYPTOKEY? ? OR CRYPTKEY? ? OR PERMITKEY? ? OR ACCESSKEY? ? OR KEYPAIR? ? OR
ASYMMETRIC?()CRYPTOGRAPHY
S6         348    S MODULAR()EXPONENTIATION
S7       97332    S CRT OR CHINESE()RESIDUE()THEOREM
S8        8051    S RSA OR RIVEST()SHAMIR()ADLEMAN
S9          53    S S4 AND (S5:S8)
S10         53    IDPAT (sorted in duplicate/non-duplicate order)
S11         44    IDPAT (primary/non-duplicate records only)
S12          6    S S11 NOT AY>2001
S13          2    S S11 NOT PY>2001
S14          6    S S12 OR S13
 ; show files
```

[File 347] **JAPIO** Dec 1976-2006/Nov(Updated 070228)

[File 348] **EUROPEAN PATENTS** 1978-2007/ 200708

**File 348: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 349] **PCT FULLTEXT** 1979-2007/UB=20070301UT=20070222

**File 349: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 350] **Derwent WPIX** 1963-2006/UD=200716

**File 350: DWPI has been enhanced to extend content and functionality of the database. For more info, visit http://www.dialog.com/dwpi/.*

14/5/1 (Item 1 from file: 349) **Links**
PCT FULLTEXT

00915099
METHOD AND DEVICE FOR DETECTING A KEY PAIR AND FOR GENERATING RSA KEYS
PROCEDE ET DISPOSITIF POUR DETERMINER UNE PAIRE DE CLES ET POUR PRODUIRE DES CLES **RSA**
VERFAHREN UND VORRICHTUNG ZUM ERMITTELN EINES SCHLUESSELPAARS UND ZUM ERZEUGEN VON **RSA**-SCHLUESSELN

Patent Applicant/Patent Assignee:

- **INFINEON TECHNOLOGIES AG**; St.-Martin-Str. 53, 81669 Munchen
  DE; DE(Residence); DE(Nationality)
  (For all designated states except: US)
- **SEIFERT Jean-Pierre; Harsdoerfer Str. 1, 81669 Munchen**
  DE; DE(Residence); DE(Nationality)
  (Designated only for: US)

Patent Applicant/Inventor:

- **SEIFERT Jean-Pierre**
  Harsdoerfer Str. 1, 81669 Munchen; DE; DE(Residence); DE(Nationality); (Designated only for: US)

Legal Representative:

- **SCHOPPE Fritz(et al)(agent)**
  Schoppe, Zimmermann, Stockeler & Zinkler, Postfach 71 08 67, 81458 Munchen; DE;

	Country	Number	Kind	Date
Patent	WO	200249266	A2-A3	20020620
Application	WO	2001EP14350		20011206
Priorities	DE	10061697		20001212

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LU; MC; NL; PT; SE; TR;

[OA] BF; BJ; CF; CG; CI; CM; GA; GN; GQ; GW;
ML; MR; NE; SN; TD; TG;

[AP] GH; GM; KE; LS; MW; MZ; SD; SL; SZ; TZ;
UG; ZM; ZW;

[EA] AM; AZ; BY; KG; KZ; MD; RU; TJ; TM;

Main International Patent Classes (Version 7):

IPC	Level
H04L-009/30	Main

Publication Language: German
Filing Language: German
Fulltext word count: 3314

English Abstract:

The invention relates to a method for detecting a number pair comprising a first number and a second number. According to the inventive method, the first number is selected (100), said first number being a first key and the second number being a second key of an encryption system, the second number being the multiplicative inverse with respect to a module of the first number, and the module equaling the product from a first prime number and a second prime number. A first subnumber (d"sub"p) and a second subnumber (d"sub"q) are calculated for the second number (d) as the multiplicative inverse of the first number (e) with respect to a second submodule (120), the first submodule and the second submodule being relatively prime. Finally, the second number (d) is determined using the first subnumber (d"sub"p) and the second subnumber (d"sub"q) and applying the Chinese remainder theorem (130).

French Abstract:

L'invention concerne un procede pour determiner une paire de nombres comprenant un premier et un deuxieme nombre, le premier nombre pouvant etre une premiere cle et le deuxieme nombre une deuxieme cle d'un systeme de codage, et le deuxieme nombre etant l'inverse multiplicatif d'un module du premier nombre, ce module etant egal au produit d'un premier nombre premier et d'un deuxieme nombre premier. Selon ce procede, on commence par selectionner (100) le premier nombre, puis on calcule (110) un premier sous-nombre (d"sub"p) pour le deuxieme nombre (d) comme inverse multiplicatif du premier nombre (e) par rapport a un premier sous-module egal au premier nombre premier moins 1 divise par le plus grand denominateur commun (ggT) du premier nombre premier moins 1 et du deuxieme nombre premier moins 1. On calcule (120) ensuite un deuxieme sous-nombre (d"sub"q) pour le deuxieme nombre (d) comme inverse multiplicatif du premier nombre (e) par rapport a un deuxieme sous-module egal au deuxieme nombre premier (q) moins 1, le premier et le deuxieme sous-module etant relativement premiers. Pour finir, le deuxieme nombre (d) est determine (130) a l'aide du premier sous-nombre (d"sub"p) et du deuxieme sous-nombre (d"sub"q) au moyen du theoreme chinois des restes (**CRT**). En utilisant le theoreme chinois des restes, on transforme l'operation de formation des inverses multiplicatifs en deux operations correspondantes avec des nombres plus courts et une etape de combinaison rapide, si bien que l'on obtient une acceleration de facteur 4 comparativement a un procede ne faisant pas appel au theoreme chinois des restes.

Type	Pub. Date	Kind	Text
Publication	20020620	A2	Without international search report and to be republished upon receipt of that report.
Search Rpt	20021227		Late publication of international search report
Republication	20021227	A3	With international search report.
Examination	20030213		Request for preliminary examination prior to end of 19th month from priority date

14/5/2 (Item 2 from file: 349) **Links**
PCT FULLTEXT

00884964
METHOD AND DEVICE FOR CARRYING OUT A MODULAR EXPONENTIATION IN A CRYPTOGRAPHIC PROCESSOR
PROCEDE ET DISPOSITIF PERMETTANT D'EXECUTER UNE EXPONENTIATION MODULAIRE DANS UN PROCESSEUR CRYPTOGRAPHIQUE
VERFAHREN UND VORRICHTUNG ZUM DURCHFUHREN EINER MODULAREN EXPONENTIATION IN EINEM KRYPTOGRAPHISCHEN PROZESSOR

Patent Applicant/Patent Assignee:

- **INFINEON TECHNOLOGIES AG**; St.-Martin-str. 53, 81669 Munchen
  DE; DE(Residence); DE(Nationality)
  (For all designated states except: US)
- **SEDLAK Holger**; Neumunster 10a, 85658 Egmating
  DE; DE(Residence); DE(Nationality)
  (Designated only for: US)
- **SEIFERT Jean-Pierre; Harsdorfer Str. 1, 81669 Munchen**
  DE; DE(Residence); DE(Nationality)
  (Designated only for: US)

Patent Applicant/Inventor:

- **SEDLAK Holger**
  Neumunster 10a, 85658 Egmating; DE; DE(Residence); DE(Nationality); (Designated only for: US)
- **SEIFERT Jean-Pierre**
  Harsdorfer Str. 1, 81669 Munchen; DE; DE(Residence); DE(Nationality); (Designated only for: US)

Legal Representative:

- **SCHOPPE Fritz(et al)(agent)**
  Postfach 71 08 67, 81458 Munchen; DE;

	Country	Number	Kind	Date
Patent	WO	200219065	A2	20020307
Application	WO	2001EP9285		20010810
Priorities	DE	10042234		20000828

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

[EP] AT; BE; CH; CY; DE; DK; ES; FI; FR; GB;
GR; IE; IT; LU; MC; NL; PT; SE; TR;

Main International Patent Classes (Version 7):

IPC	Level
G06F-001/00	Main
G06F-007/72	

Publication Language: German
Filing Language: German
Fulltext word count: 4032

English Abstract:

French Abstract:

Type	Pub. Date	Kind	Text
Publication	20020307	A2	Without international search report and to be republished upon receipt of that report.
Declaration	20020926		Late publication under Article 17.2a
Republication	20020926	A2	With declaration under Article 17(2)(a); without abstract; title not checked by the International Searching Authority.
Examination	20021128		Request for preliminary examination prior to end of 19th month from priority date

14/5/3 (Item 3 from file: 349) Links
PCT FULLTEXT

00516888
CODE EXCHANGE PROTOCOL
PROTOCOLE D'ECHANGE DE CODES

Patent Applicant/Patent Assignee:

- **SIEMENS AKTIENGESELLSCHAFT**;
  ; ;
- **VON DER HEIDT Guido**;
  ; ;
- **SoHNE Peter**;
  ; ;
- **VELTEN Joachim**;
  ; ;

	Country	Number	Kind	Date
Patent	WO	9948240	A1	19990923
Application	WO	99DE771		19990318
Priorities	DE	19811833		19980318

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)

Main International Patent Classes (Version 7):

IPC	Level
H04L-009/08	Main

Publication Language: German
Filing Language:
Fulltext word count: 1498

English Abstract:

The invention relates to a code exchange protocol in which communication partners (A, B) each have a secret code (S) and a public code (P). According to the invention, communication partner (A) selects a random number (x), and communication partner (B) selects a random number (y). A first partial code (Ax) is formed by communication partner (A), and a second partial code (By) is formed by communication partner (B) by using the public code (P) of the respective partner (B, A). Each partial code is transmitted to the other communication partner (B, A). A session code (gxy, gyx) is formed from each of the personal random numbers (x, y) and from the partial code (By, Ax) of the respective communication partner (B, A) by using the personal secret code (S), whereby the partial codes (Ax, By), and the session codes (gxy, gyx) can be calculated in a manner which is analogous to the Diffie-Hellman protocol.

French Abstract:

L'invention concerne un protocole d'echange de codes dans lequel des correspondants (A, B) possedent respectivement un code secret (S) et un code public (P), le correspondant (A) composant un nombre aleatoire (x) et le correspondant (B) composant un nombre aleatoire (y). Un premier code partiel (Ax) est forme par le correspondant (A), et un deuxieme code partiel (By) est forme par le correspondant (B) a l'aide du code public (P) du correspondant respectif (B, A), ce premier code et ce deuxieme code etant transmis respectivement a l'autre correspondant (B, A). Un code de session (gxy, gyx) est forme respectivement a partir du nombre aleatoire personnel (x, y) et du code partiel (By, Ax) du correspondant respectif (B, A), a l'aide du code secret (S) personnel, le code partiel (Ax, By) et le code de session (gxy, gyx) etant calcules par analogie avec le protocole de Diffie-Hellman.

14/5/4 (Item 1 from file: 350) **Links**
Derwent WPIX

0012395983 *Drawing available*
WPI Acc no: 2002-339681/200237
XRPX Acc No: N2002-267108
Method for production of security module with virtual memory addressing uses provision of 2 security modules having different mapping specifications
Patent Assignee: INFINEON TECHNOLOGIES AG (INFN)
Inventor: SEDLAK H; **SEIFERT J**

Patent Family (5 patents, 93 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
WO 2002019065	A2	20020307	WO 2001EP9285	A	20010810	200237	B
DE 10042234	A1	20020314	DE 10042234	A	20000828	200237	E
DE 10042234	C2	20020620	DE 10042234	A	20000828	200239	E
AU 200187675	A	20020313	AU 200187675	A	20010810	200249	E
AU 2001287675	A8	20050922	AU 2001287675	A	20010810	200570	E

Priority Applications (no., kind, date): DE 10042234 A 20000828

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
WO 2002019065	A2	DE	26	5		
National Designated States,Original	AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW					
Regional Designated States,Original	AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR					
AU 200187675	A	EN			Based on OPI patent	WO 2002019065
AU 2001287675	A8	EN			Based on OPI patent	WO 2002019065

Alerting Abstract WO A2
NOVELTY - The method uses provision of a first security module with a first mapping specification for mapping logical addresses onto physical addresses and provision of a second security module with a second mapping specification, which is different to the first mapping specification, with random provision of the first or the second mapping specification.
DESCRIPTION - Also included are INDEPENDENT CLAIMS for the following:

A. a security module with virtual memory addressing;
B. a device for production of a security module with virtual memory addressing;
C. a method for configuring a security module with a virtual memory address

USE - The method is used for production of a security module with virtual memory addressing.
ADVANTAGE - The stored information is stored in different physical addresses at 2 different points in time for increasing the protection of the security module from attack.
DESCRIPTION OF DRAWINGS - The figure shows a flow diagram for production of a security module with virtual memory addressing. (Drawing includes non-English language text).

Title Terms /Index Terms/Additional Words: METHOD; PRODUCE; SECURE; MODULE; VIRTUAL; MEMORY; ADDRESS; PROVISION; MAP; SPECIFICATION

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-001/00; H04L-009/30			Main		"Version 7"
G06F-007/58; G06F-007/72			Secondary		"Version 7

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-H01A; T01-H01C2; T01-H03A; T01-J12C

DE 59906682	G	DE			Application	EP 1999919098
					PCT Application	WO 1999DE771
					Based on OPI patent	EP 1062763
					Based on OPI patent	WO 1999048240
US 7016500	B1	EN			PCT Application	WO 1999DE771
					Based on OPI patent	WO 1999048240

Alerting Abstract WO A1

NOVELTY - Communications partner A selects random number x and partner B selects number y. Subcodes Ax for partner A and By for partner B are set up by using a public code P. Each subcode is transmitted to the other partner. Sessions codes gxy and gyx are set up from both the random numbers x and y and from subcodes Ax and By by using a personal secret code S. This allows subcodes Ax and By along with session codes gxy and gyx to be calculated to match the Diffie-Hellman protocol.
USE - In end-to-end authentification. In encoding procedures, coding devices and tamper-proof devices.
ADVANTAGE - The encoding procedure requires little computation, since little exponential application is needed.

Title Terms /Index Terms/Additional Words: CODE; EXCHANGE; PROTOCOL; COMMUNICATE; PARTNER

Class Codes

International Patent Classification

IPC	**Class Level**	**Scope**	**Position**	**Status**	**Version Date**
H04L-009/08; H04L-009/30			Main		"Version 7"
G09C-001/00			Secondary		"Version 7
H04L-0009/00	A	I	F	B	20060101

US Classification, Issued: 380282000, 380030000, 380046000, 713171000

File Segment: EngPI; EPI;
DWPI Class: T01; W01; P85
Manual Codes (EPI/S-X): T01-D01; T01-J12C; W01-A05A; W01-A05B

1/5/1 **Links**
Derwent WPIX

Your App

0013194811 *Drawing available*
WPI Acc no: 2003-278924/200327
XRPX Acc No: N2003-221446

Calculation of the result of a modular exponentiation to increase RSA-CRT calculation security against cryptographic attacks by randomization of the auxiliary exponents or alteration of the sub- modules

Patent Assignee: INFINEON TECHNOLOGIES AG (INFN)
Inventor: SEIFERT J; SEIFERT J P; VELTEN J

Patent Family (7 patents, 100 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
WO 2003023605	A2	20030320	WO 2002EP9405	A	20020822	200327	B
DE 10143728	A1	20030403	DE 10143728	A	20010906	200330	E
EP 1423786	A2	20040602	EP 2002797920	A	20020822	200436	E
			WO 2002EP9405	A	20020822		
DE 10143728	B4	20040902	DE 10143728	A	20010906	200457	E
AU 2002333678	A1	20030324	AU 2002333678	A	20020822	200460	E
US 20040215685	A1	20041028	WO 2002EP9405	A	20020822	200471	E
			US 2004789373	A	20040227		
CN 1554047	A	20041208	CN 2002817557	A	20020822	200517	E

Priority Applications (no., kind, date): DE 10143728 A 20010906

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
WO 2003023605	A2	DE	24	3		
National Designated States,Original	AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW					
Regional Designated States,Original	AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SK SL SZ TR TZ UG ZM ZW					
EP 1423786	A2	DE			PCT Application	WO 2002EP9405
					Based on OPI patent	WO 2003023605
Regional Designated States,Original	AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR					
AU 2002333678	A1	EN			Based on OPI patent	WO 2003023605
US 20040215685	A1	EN			Continuation of application	WO 2002EP9405

Inventor's NPL

```
Set      Items    Description
S1        1806    S AU=(SEIFERT, J? OR SEIFERT J?)
S2         828    SELECT AU= "SEIFERT, J" OR AU= "SEIFERT, J."
S3          40    SELECT AU= "SEIFERT, J.-P." OR AU= "SEIFERT, J.P."
S4          19    SELECT AU= "SEIFERT, JEAN-PIERRE"
S5         582    SELECT AU= "SEIFERT J"
S6          23    SELECT AU= "SEIFERT J P" OR AU= "SEIFERT JP"
S7           7    SELECT AU= "SEIFERT JEAN-PIERRE"
S8        1499    S S2:S7
S9          91    S AU=(VELTEN, J? OR VELTEN J?)
S10       1590    S S8 OR S9
S11      35550    S (PUBLIC OR SECRET OR PRIVATE OR ENCRYPT? OR CRYPT?)()KEY? ? OR PKI OR
CRYPTOKEY? ? OR CRYPTKEY? ? OR PERMITKEY? ? OR ACCESSKEY? ? OR KEYPAIR? ? OR
ASYMMETRIC?()CRYPTOGRAPHY
S12     791626    S ENCRYPT? OR CIPHER? OR CYPHER? OR CRYPTO? OR ENCIPHER? OR ENCYPHER? OR
ENCOD?
S13       7451    S S12 AND (RSA OR CRT)
S14          3    S CHINESE()RESIDUE()THEOREM
S15       1875    S CHINESE()REMAINDER()THEOREM
S16        375    S RIVEST()SHAMIR()ADLEMAN
S17       1118    S MODULAR()EXPONENTIATION
S18         38    S S10 AND (S11 OR S13 OR S14 OR S15 OR S16 OR S17)
S19          9    S S18 NOT PY>2001
S20          5    RD  (unique items)
 ; show files
```

[File 8] **Ei Compendex(R)** 1884-2007/Feb W4

[File 35] **Dissertation Abs Online** 1861-2007/Feb

[File 65] **Inside Conferences** 1993-2007/Mar 07

[File 2] **INSPEC** 1898-2007/Feb W4

[File 94] **JICST-EPlus** 1985-2007/Mar W2

**File 94: UD200609W2 is the last update for 2006. UD200701W1 is the first update for 2007. The file is complete and up to date.*

[File 111] **TGG Natl.Newspaper Index(SM)** 1979-2007/Mar 05

[File 6] **NTIS** 1964-2007/Mar W1

[File 144] **Pascal** 1973-2007/Feb W4

[File 434] **SciSearch(R) Cited Ref Sci** 1974-1989/Dec

[File 34] **SciSearch(R) Cited Ref Sci** 1990-2007/Mar W1

[File 62] **SPIN(R)** 1975-2007/Feb W3

[File 99] **Wilson Appl. Sci & Tech Abs** 1983-2007/Feb

[File 95] **TEME-Technology & Management** 1989-2007/Mar W1

[File 56] **Computer and Information Systems Abstracts** 1966-2007/Feb

[File 57] **Electronics & Communications Abstracts** 1966-2007/Feb

[File 60] **ANTE: Abstracts in New Tech & Engineer** 1966-2007/Feb

[File 266] **FEDRIP** 2007/Feb

[File 583] **Gale Group Globalbase(TM)** 1986-2002/Dec 13

**File 583: This file is no longer updating as of 12-13-2002.*

[File 239] **Mathsci** 1940-2007/Apr

20/5/1 (Item 1 from file: 2) **Links**
INSPEC

08087050 **INSPEC Abstract Number:** B2001-12-6120D-066, C2001-12-1260C-037
Title: Using fewer qubits in Shor's factorization algorithm via simultaneous Diophantine approximation
Author Seifert, J.-P.
Author Affiliation: Infineon Technol., Munich, Germany
Conference Title: Topics in Cryptology - CT-RSA 2001. The Cryptographers' Track at RSA Conference 2001. Proceedings (Lecture Notes in Computer Science Vol.2020) p. 319-27
Editor(s): Naccache, D.
Publisher: Springer-Verlag , Berlin, Germany
Publication Date: 2001 **Country of Publication:** Germany xii+471 pp.
ISBN: 3 540 41898 9 **Material Identity Number:** XX-2001-01772
Conference Title: Topics in Cryptology - CT-RSA 20001
Conference Sponsor: Compaq Comput. Corp.; Hewlett-Packard; IBM; Intel Corp.; Microsoft; nCipher ; EDS; et al
Conference Date: 8-12 April 2001 **Conference Location:** San Francisco, CA, USA

Language: English **Document Type:** Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: While quantum computers might speed up in principle certain computations dramatically, in practice, though quantum computing technology is still in its infancy. Even we cannot clearly envision at present what the hardware of that machine will be like. Nevertheless, we can be quite confident that it will be much easier to build any practical quantum computer operating on a few number of quantum bits rather than one operating on a huge number of quantum bits. It is therefore of big practical impact to use the resource of quantum bits very sparingly, ie, to find quantum algorithms which use as few as possible quantum bits. Here, we present a method to reduce the number of actually needed qubits in Shor's algorithm to factor a composite number N. Exploiting the inherent probabilism of quantum computation we are able to substitute the continued fraction algorithm to find a certain unknown fraction by a simultaneous Diophantine approximation. While the continued fraction algorithm is able to find a Diophantine approximation to a single known fraction with a denominator greater than N/sup 2/, our simultaneous Diophantine approximation method computes in polynomial time unusually good approximations to known fractions with a denominator of size N/sup 1+ epsilon /, where epsilon is allowed to be an arbitrarily small positive constant. As these unusually good approximations are almost unique we are able to recover an unknown denominator using fewer qubits in the quantum part of our algorithm. (26 Refs)
Subfile: B C
Descriptors: computational complexity; number theory; **public key** cryptography; quantum computing; quantum cryptography
Identifiers: Shor factorization algorithm; simultaneous Diophantine approximation; quantum computers; quantum computing; quantum bits; quantum algorithms; qubits; probabilism; continued fraction algorithm; polynomial time
Class Codes: B6120D (Cryptography); B0250 (Combinatorial mathematics); C1260C (Cryptography theory); C4270 (Quantum computing theory); C1160 (Combinatorial mathematics)

20/5/2 (Item 2 from file: 2) **Links**

INSPEC

07670476 **INSPEC Abstract Number:** B2000-09-6120D-039, C2000-09-1260C-022

Title: Extending Wiener's attack in the presence of many decrypting exponents

Author Howgrave-Graham, N.; **Seifert, J.-P.**

Author Affiliation: Math. Sci. Dept., Bath Univ., UK

Conference Title: Secure Networking - CQRE [Secure]'99. International Exhibition and Congress. Proceedings (Lecture Notes in Computer Science Vol.1740) p. 153-66

Editor(s): Baumgart, R.

Publisher: Springer-Verlag , Berlin, Germany

Publication Date: 1999 **Country of Publication:** Germany ix+258 pp.

ISBN: 3 540 66800 4 **Material Identity Number:** XX-2000-00034

Conference Title: Secure Networking - CQRE [Secure]'99

Conference Date: 30 Nov.-2 Dec. 1999 **Conference Location:** Dusseldorf, Germany

Language: English **Document Type:** Conference Paper (PA)

Treatment: Theoretical (T)

Abstract: Wiener (1990) has shown that when the **RSA** protocol is used with a decrypting exponent, d, which is less than N/sup 1/4/ and an **encrypting** exponent, e, approximately the same size as N, then d can usually be found from the continued fraction approximation of e/N. We extend this attack to the case when there are many e/sub i/ for a given N, all with small d/sub i/. For the case of two such e/sub i/, the d/sub i/ can (heuristically) be as large as N/sup 5/14/ and still be efficiently recovered. As the number of **encrypting** exponents increases the bound on the d/sub i/, which enables efficient recovery of the d/sub i/, increases (slowly) to N/sup 1- epsilon /. However, the complexity of our method is exponential in the number of exponents present, and therefore only practical for a relatively small number of them. (12 Refs)

Subfile: B C

Descriptors: protocols; **public key cryptography**

Identifiers: decrypting exponents; **RSA** protocol; **encrypting** exponent; fraction approximation; exponential complexity; **public key cryptography**

Class Codes: B6120D (Cryptography); C1260C (Cryptography theory); C6130S (Data security)

20/5/3 (Item 3 from file: 2) **Links**
INSPEC

07576378 **INSPEC Abstract Number:** B2000-06-6120D-020, C2000-06-1260C-019
Title: Tensor-based trapdoors for CVP and their application to public key cryptography
Author Fischlin, R.; **Seifert, J.-P.**
Author Affiliation: Fachbereich Math., Frankfurt Univ., Germany
Conference Title: Cryptography and Coding. 7th IMA International Conference. Proceedings (Lecture Notes in Computer Science Vol.1746) p. 244-57
Editor(s): Walker, M.
Publisher: Sprnger-Verlag , Berlin, Germany
Publication Date: 1999 **Country of Publication:** Germany ix+312 pp.
ISBN: 3 540 66887 X **Material Identity Number:** XX-1998-03682
Conference Title: Proceedings of 7th Conference on Cryptography and Coding
Conference Date: 20-22 Dec. 1999 **Conference Location:** Cirencester, UK

Language: English **Document Type:** Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: We propose two trapdoors for the closest-vector-problem in lattices (CVP) related to the lattice tensor product. Using these trapdoors we set up a lattice-based cryptosystem which resembles the McEliece scheme. (26 Refs)
Subfile: B C
Descriptors: lattice theory; **public key** cryptography; tensors; vectors
Identifiers: tensor-based trapdoors; **public key** cryptography; closest-vector problem; lattice tensor product
Class Codes: B6120D (Cryptography); B0210 (Algebra); C1260C (Cryptography theory); C1110 (Algebra)

20/5/4 (Item 1 from file: 144) **Links**
Fulltext available through: USPTO Full Text Retrieval Options ScienceDirect
Pascal

15333989 PASCAL No.: 02-0020666

Information leakage attacks against Smart card implementations of the elliptic curve digital signature algorithm
E-smart 2001 : smart card programming and security : Cannes, 19-21 September 2001

ROEMER Tanja; **SEIFERT Jean-Pierre**
ATTALI Isabelle, ed; JENSEN Thomas, ed
Infineon Technologies Corporation Security & ChipCard ICs Technical Innovations, 81609 Munich, Germany
International conference on research in smart cards (Cannes FRA) 2001-09-19
Journal: Lecture notes in computer science,
2001, 2140 211-219

ISBN: 3-540-42610-8 ISSN: 0302-9743 Availability: INIST-16343; 354000097048760170
No. of Refs.: 18 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English
In this article we will be concerned with a polynomial-time attack against the ECDSA, which computes the **secret key** of the ECDSA if a few bits of the ephemeral-key from several ECDSA-signatures are known. The number of needed bits per signature is 12, if one has access to an ideal lattice basis reduction algorithm computing the n SUP t SUP h successive minimum of a lattice with rank n. The aforesaid bits of the ephemeral-key can be obtained from insecure ECDSA implementations by so called side-channel-attacks like Timing, Simple-Power-Analysis, Differential-Power-Analysis, Electromagnetic or Differential-Fault attacks. Our attack combines a recent idea of Howgrave-Graham and Smart with an old lattice attack against linear congruential pseudo-random number generators due to Frieze, Hastad, Kannan, Lagarias und Shamir. In contrast to Howgrave-Graham and Smart, our approach enables the exact determination of the number of needed (side-channel) bits and uses an easier lattice problem making the attack very practical.

English Descriptors: Cryptanalysis; Fault diagnostic; Timing; Elliptic curve; Intelligent system; Digital signature; Smart cards; Polynomial time; Lattice

French Descriptors: Cryptanalyse; Diagnostic panne; Timing; Courbe elliptique; Systeme intelligent; Signature numerique; Carte a puce; Temps polynomial; Treillis; Smart card

Classification Codes: 001D04A04E

20/5/5 (Item 1 from file: 239) **Links**
Mathsci

03301702 **MR** 2002h#94079
Tensor-based trapdoors for CVP and their application to public key cryptography (extended abstract).

Cryptography and coding (Cirencester, 1999)
Fischlin, Roger (Department of Mathematics, Johann Wolfgang Goethe-Universitat Frankfurt, D-60054 Frankfurt am Main, Germany)
Seifert, Jean-Pierre (Department of Mathematics, Johann Wolfgang Goethe-Universitat Frankfurt, D-60054 Frankfurt am Main, Germany)
Corporate Source Codes: D-FRNK; D-FRNK
1999 ,
Springer, Berlin, ; 244--257, ,
Series: Lecture Notes in Comput. Sci., 1746,
Language: English **Summary Language:** English
Document Type: Proceedings Paper
Journal Announcement: 200203
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: SHORT (4 lines)
Summary: ``We propose two trapdoors for the closest-vector problem in lattices related to the lattice tensor product. Using these trapdoors we set up a lattice-based cryptosystem which resembles the McEliece scheme."
\{For the entire collection see MR 2002d:94047.\}
Reviewer: Summary
Review Type: Abstract
Proceedings Reference: 2002d#94047 ; 1 861 825
Descriptors: * 94A62 -Information and communication, circuits-Communication, information- Authentication and secret sharing

```
Set      Items    Description
S1       15291    S (PRIVATE OR SECRET)()KEY? ? OR ASYMMETRIC?()CRYPTOGRAPHY
S2         346    S MODULAR()EXPONENTIATION
S3       73049    S CRT OR CHINESE()(RESIDUE OR REMAINDER)()THEOREM
S4         442    S (EIGHTH OR 8TH ) (3W) (QUANTITY OR QUANTITIES OR SUM OR SUMS OR TOTAL? ?
OR RESULT? ? )
S5        2807    S PRIME()NUMBER? ?
S6       26273    S (RANDOM OR PSEUDORANDOM)()(NUMBER? ? OR INTEGER? ? OR VALUE? ?)
S7        5806    S (SAFETY OR SECURITY) () (PARAMETER? ? OR NUMBER? ? OR VALUE? ?)
S8           0    S S1 (50N) S2 (50N) S3 (50N) S4 (50N) S5 (50N) S6 (50N) S7
S9        2387    S (AUTHORI? OR AUTHENTICAT?)() (PARAMETER? ? OR NUMBER? ? OR VALUE? ?)
S10          0    S S1 (50N) S2 (50N) S3 (50N) S4 (50N) S5 (50N) S6 (50N) S9
S11          0    S S1 (50N) S2 (50N) S4 (50N) S5 (50N) S6 (50N) (S7 OR S9)
 ; show files
```

[File 348] **EUROPEAN PATENTS** 1978-2007/ 200708

**File 348: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 349] **PCT FULLTEXT** 1979-2007/UB=20070308UT=20070301

**File 349: For important information about IPCR/8 and forthcoming changes to the IC= index, see HELP NEWSIPCR.*

[File 350] **Derwent WPIX** 1963-2006/UD=200716

**File 350: DWPI has been enhanced to extend content and functionality of the database. For more info, visit http://www.dialog.com/dwpi/.*

```
Set      Items   Description
S1        1613   S (PRIVATE OR SECRET)()KEY? ? OR ASYMMETRIC?()CRYPTOGRAPHY
S2           2   S MODULAR()EXPONENTIATION
S3           0   S S1 AND S2
 ; show files
```

[File 347] **JAPIO** Dec 1976-2006/Nov(Updated 070228)

```
Set       Items    Description
S1         8870    S (PRIVATE OR SECRET)()KEY? ? OR ASYMMETRIC?()CRYPTOGRAPHY
S2         1118    S MODULAR()EXPONENTIATION
S3        35826    S CRT OR CHINESE()(RESIDUE OR REMAINDER)()THEOREM
S4          361    S (EIGHTH OR 8TH ) (3W) (QUANTITY OR QUANTITIES OR SUM OR SUMS OR TOTAL? ?
OR RESULT? ? )
S5        12337    S PRIME()NUMBER? ?
S6        26182    S (RANDOM OR PSEUDORANDOM)()(NUMBER? ? OR INTEGER? ? OR VALUE? ?)
S7         3431    S (SAFETY OR SECURITY) () (PARAMETER? ? OR NUMBER? ? OR VALUE? ?)
S8            0    S S1 AND S2 AND S3 AND S4 AND S5 AND S6 AND S7
S9          166    S (AUTHORI? OR AUTHENTICAT?) () (PARAMETER? ? OR NUMBER? ? OR VALUE? ?)
S10           0    S S1 AND S2 AND S3 AND S4 AND S5 AND S6 AND S9
S11           0    S S1 AND S2 AND S4 AND S5 AND S6 AND (S7 OR S9)
 ; show files
```

[File 8] **Ei Compendex(R)** 1884-2007/Feb W4

[File 35] **Dissertation Abs Online** 1861-2007/Feb

[File 65] **Inside Conferences** 1993-2007/Mar 07

[File 2] **INSPEC** 1898-2007/Feb W4

[File 94] **JICST-EPlus** 1985-2007/Mar W2

**File 94: JICST will be removed from all vendors on March 31, 2007. Please contact the Knowledge Center for alternative files.*

[File 111] **TGG Natl.Newspaper Index(SM)** 1979-2007/Mar 06

[File 6] **NTIS** 1964-2007/Mar W1

[File 144] **Pascal** 1973-2007/Feb W4

[File 434] **SciSearch(R) Cited Ref Sci** 1974-1989/Dec

[File 34] **SciSearch(R) Cited Ref Sci** 1990-2007/Mar W1

[File 62] **SPIN(R)** 1975-2007/Feb W3

[File 99] **Wilson Appl. Sci & Tech Abs** 1983-2007/Feb

[File 95] **TEME-Technology & Management** 1989-2007/Mar W1

[File 56] **Computer and Information Systems Abstracts** 1966-2007/Feb

[File 57] **Electronics & Communications Abstracts** 1966-2007/Feb

[File 60] **ANTE: Abstracts in New Tech & Engineer** 1966-2007/Feb

[File 266] **FEDRIP** 2007/Feb

[File 583] **Gale Group Globalbase(TM)** 1986-2002/Dec 13

**File 583: This file is no longer updating as of 12-13-2002.*

[File 239] **Mathsci** 1940-2007/Apr

```
Set     Items    Description
S1      15284    S (PRIVATE OR SECRET)()KEY? ? OR ASYMMETRIC?()CRYPTOGRAPHY
S2        131    S MODULAR()EXPONENTIATION
S3      85255    S CRT OR CHINESE()(RESIDUE OR REMAINDER)()THEOREM
S4       3168    S (EIGHTH OR 8TH ) (3W) (QUANTITY OR QUANTITIES OR SUM OR SUMS OR TOTAL? ?
OR RESULT? ? )
S5       3525    S PRIME()NUMBER? ?
S6      12815    S (RANDOM OR PSEUDORANDOM)()(NUMBER? ? OR INTEGER? ? OR VALUE? ?)
S7      66283    S (SAFETY OR SECURITY OR AUTHORI? OR AUTHENTICAT?) () (PARAMETER? ? OR
NUMBER? ? OR VALUE? ?)
S8          0    S S1 (50N) S2 (50N) S3 (50N) S4 (50N) S5 (50N) S6 (50N) S7
S9          0    S S1 (50N) S2 (50N) S4 (50N) S5 (50N) S6 (50N) S7
 ; show files
```

[File 369] **New Scientist** 1994-2007/Nov W2

[File 160] **Gale Group PROMT(R)** 1972-1989

[File 635] **Business Dateline(R)** 1985-2007/Mar 07

[File 15] **ABI/Inform(R)** 1971-2007/Mar 08

[File 16] **Gale Group PROMT(R)** 1990-2007/Mar 08

[File 9] **Business & Industry(R)** Jul/1994-2007/Mar 08

[File 810] **Business Wire** 1986-1999/Feb 28

[File 610] **Business Wire** 1999-2007/Mar 09

**File 610: File 610 now contains data from 3/99 forward. Archive data (1986-2/99) is available in File 810.*

[File 647] **CMP Computer Fulltext** 1988-2007/May W3

[File 98] **General Sci Abs** 1984-2007/Mar

[File 148] **Gale Group Trade & Industry DB** 1976-2007/Feb 28

[File 634] **San Jose Mercury** Jun 1985-2007/Mar 08

[File 275] **Gale Group Computer DB(TM)** 1983-2007/Mar 08

[File 47] **Gale Group Magazine DB(TM)** 1959-2007/Feb 28

[File 75] **TGG Management Contents(R)** 86-2007/Feb W4

[File 636] **Gale Group Newsletter DB(TM)** 1987-2007/Mar 08

[File 624] **McGraw-Hill Publications** 1985-2007/Mar 09

**File 624: Homeland Security & Defense and 9 Platt energy journals added Please see HELP NEWS624 for more*

[File 484] **Periodical Abs Plustext** 1986-2007/Feb W3

[File 613] **PR Newswire** 1999-2007/Mar 09

**File 613: File 613 now contains data from 5/99 forward. Archive data (1987-4/99) is available in File 813.*

[File 813] **PR Newswire** 1987-1999/Apr 30

[File 141] **Readers Guide** 1983-2007/Jan

[File 370] **Science** 1996-1999/Jul W3

**File 370: This file is closed (no updates). Use File 47 for more current information.*

[File 696] **DIALOG Telecom. Newsletters** 1995-2007/Mar 08

[File 553] **Wilson Bus. Abs.** 1982-2007/Mar

[File 621] **Gale Group New Prod.Annou.(R)** 1985-2007/Feb 28

[File 674] **Computer News Fulltext** 1989-2006/Sep W1

**File 674: File 674 is closed (no longer updates).*

[File 20] **Dialog Global Reporter** 1997-2007/Mar 09

Google Scholar BETA | ("private key" OR "asymmetric cryptography") | 1800 - 2001 | Search | Adv Sch Sch

Lowercase **"or"** was ignored. Try **"OR"** to search for either of two terms. [details]

Scholar Results **1** - **3** of **3** for **("private key" OR "asymmetric cryptography") "modular exponentiation" "**

All Results

T Wu

M Roe

Tip: Try removing quotes from your search to get more results.

The secure remote password protocol - group of 56 »
T Wu... - ... Internet Society Network and Distributed System **Security** ..., 1998 - downloads.securityfocus.com
... copy of the user's password or **private key** is known ... GF n . In other words, a large **prime number** n ... verier-generator P becomes a **modular exponentiation** in GF ...
Cited by 217 - Related Articles - View as HTML - Web Search

[BOOK] Secure Communicating Systems: Design, Analysis, and Implementation
M Huth - 2001 - books.google.com
... and analysis ofcryptographic systems, **security** protocols, and programs that process secret or confidential information — together with the **safety** analysis of ...
Cited by 2 - Related Articles - Web Search - Library Search

Cryptography and Evidence - group of 13 »
M Roe - Doct. Dissert., Univ of Cambridge, UK, 1997 - research.microsoft.com
... 46 6.1.1 Distinction between a **security** problem and a reliability problem ....
52 7 The Lifecycle of a **Private Key** 53 7.1 The Enemy Within ....
Cited by 31 - Related Articles - View as HTML - Web Search

("private key" OR "asymmetric crypt(Search

Google Home - About Google - About Google Scholar

ip.com IP.com PriorArtDatabase
Securing innovation

March 09, 2007 USPTO

Search
- Full Text
- Concept
- Document ID
- Recent Disclosures

Other
- Prior Art Home
- Support
- Logout

Displaying records #1 through 1 out of 1

Result # 1 Relevance: ○○○○○

The OAKLEY Key Determination Protocol (RFC2412)

1998-11-01 IPCOM000002988D English (United States)

This document describes a protocol, named OAKLEY, by which two authenticated parties can agree on secure and secret keying material. The basic mechanism is the Diffie-Hellman key exchange algorithm.

Displaying page 1 of 1 << FIRST | < BACK | NEXT > | LAST >>

Search query: (private key OR asymmetric cryptography) AND modular exponentiation AND prime number AND random number

New search | Modify this search | Search within current results

Scientific & Technical Information Center

NPL Services for Examiners

Search

My List - 0 Help

Main Search | Advanced Keyword Search | Search History

Search: Title Alphabetical | Algebraic aspects of cryptogra | GO | Refine Search

> You're searching: **Scientific and Technical Information Center**

Item Information

- Holdings

Browse Catalog

by title:

- Algebraic aspects of...

Search Bookstores

- Amazon
- Barnes and Noble

MARC Display

Algebraic aspects of cryptography /

Author:	Koblitz, Neal, 1948-
Imprint:	Berlin ; New York : Springer, c1998.
Notes:	"With an appendix on hyperelliptic curves by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato." Includes bibliographical references (p. [193]-200) and index.
ISBN:	3540634460 (hardcover : alk. paper)
Subjects:	Coding theory. Curves, Elliptic
Series:	Algorithms and computation in mathematics
Description:	ix, 206 p. : ill. ; 24 cm.

Add to my list

Copy/Holding information

Collection	Call No.	Copy	Status
EIC for TC 2100	QA268 .K585 1998	c.1	Checked out
EIC for TC 2100	QA268 .K585 1998	c.2	Checked out
EIC for TC 2100	QA268 .K585 1998	c.3	Checked out
EIC for TC 2100	QA268 .K585 1998	c.4	Available